Post-Quantum Cryptography (P-QC)

Quantum Qwyit™

Post-Quantum Crypto Failure

- NIST 6-year effort to select new P-QC algorithms for standardization
- SIKE, one of the 4 finalists, was broken right after announcement – using a PC (no quantum required!)

I asked Jao, the SIKE co-inventor, why the weakness had come to light only now, in a relatively later stage of its development. His answer was insightful:

"It's true that the attack uses mathematics which was published in the 1990s and 2000s. In a sense, the attack doesn't require new mathematics; it could have been noticed at any time. In general there is a lot of deep mathematics which has been published in the mathematical literature but which is not well understood by cryptographers. I lump myself into the category of those many researchers who work in cryptography but do not understand as much mathematics as we really should.

So sometimes all it takes is someone who recognizes the applicability of existing theoretical math to these new cryptosystems."

"It is perhaps a bit concerning that this is the second example in the past six months of a scheme that made it to the 3rd round of the NIST review process before being completely broken using a classical algorithm. (The earlier example was Rainbow.) Three of the four PQC schemes rely on relatively new assumptions whose exact difficulty is not well understood, so what the latest attack indicates is that we perhaps still need to be cautious/conservative with the standardization process going forward." – Jonathan Katz, IEEE, UMd

P-QC Must Be Post-*Computing* Crypto

"All it actually takes is someone who recognizes that *any and every cryptosystem that is computationally bound will forever be broken by any* ***computing capability.***" – Paul McGough, Qwyit CTO

There's only one type of cryptography that meets the not-computationally-bound singular, correct and *only* criteria for Post-Computing success:
Perfect Secrecy

Shannon's Perfect Secrecy (PS)

- Claude Shannon's 1948 Secrecy Systems paper (Communication Theory of Secrecy Systems) details PS
- PS is 100% unbreakable encryption – *it's not computationally bound and therefore forever safe under any computing platform:* meets the singular criteria for Post-Computing Crypto (P-CC)
- It's been wrongly abandoned – because *in Shannon's paper,* Perfect Secrecy was detailed, exampled and proven possible in *practical Strongly Ideal Systems* (finite key systems)
- No one ever *engineered* one (until Qwyit™)

Today and Tomorrow's *Practical*

- It's not enough for the system to be Strongly Ideal (Perfectly Secure). It must have specific Practical Properties:

  - *Fast:* Perform within real world communication speed w/o degradation
  - *Efficient:* Fit on any and every network device profile (HW/SW/FW), and within any and every communication bandwidth
  - *Flexible*: Work in any business process and every federated trust model

Post-Computing Crypto Summary

Cryptography is again about to go chasing imperfect systems in a P-QC world that no one can even imagine…and do it in the same way they mistakenly handled the last 75 years: full of hubris and flat-out wrong assumptions.

It's time for real cryptographic change…and success:

- There is only one P-QC/P-CC algorithm design guaranteed to work and be forever safe under any computing platform: *not-computationally-bound*
- There is only one absolute definition of any cryptography that is not computationally bound: *Perfect Secrecy*
- Cryptography has only one absolute definition of *Perfect Secrecy* in *practical* finite keyed systems: *Shannon Defined Strongly Ideal Systems*
- *Practical* means real world *Speed*, *Efficiency* and *Flexibility*

Quantum Qwyit™

- Qwyit™ is the first and only *Strongly Ideal System* meeting all of Shannon's PS requirements
- Brilliant engineering achievement using simple cryptographic primitives that include:
  - Complete Cryptosystem - Authentication and Encryption (unique QCy™ cipher)
  - Solves Crypto vulnerabilities (any and every attack profile)
  - Stops cybercrime 'edge' attacks (identity theft, network break-ins, stolen crypto-currency, etc.)
  - Performs in a single machine cycle (*Fast*)
  - In less than 300 lines of VHDL fitting on any network device profile (HW/SW/FW) (*Efficient*)
  - For any federated business and trust model (*Flexible*)

Qwyit can be Everywhere, in Everything and On All The Time

Sounds too good to be true…*but*

Test It

- Partnered with Onclave for Air Force OpenVPN project – tested, documented
- Instantiated on an FPGA – see the video here…put it in your lab
- Several SW apps (QFone – a 100% secure video&voice app) – available for review, benchmarking, cryptanalysis
- Independently tested and verified – papers, contacts
- Submitted and presented at 2015 NIST Lightweight Cryptography conference
- Reference documents, test vectors, security discussions, etc.
- Patents

100% Transparency: Method, Papers, Product, Patents – *Test It!*

Conclusions

- Cryptography must acknowledge the obvious: the hubris, imperfect algorithms, convoluted complex processes – and abysmal constant failure
- Now is a crucial juncture and opportunity to change course, and deliver a real world solution for next generation Post-Quantum/Post-Computing Cryptography's brave new world
- A Shannon-defined *Practical Perfect Secrecy Strongly Ideal System* exists for the entire future Cryptographic Universe
- Qwyit™ is 100% ready for inspection – *see for yourself!*

Further Information

All of the preceding is fully discussed in our *Quantum Qwyit*™ whitepaper – ask for it!

Contact Qwyit LLC

Mike Fortkort, Co-Founder and CEO
MikeF@Qwyit.com
www.qwyit.com info@qwyit.com

All truth passes through three stages. First, it is ridiculed. Second, it is violently opposed.

Third, it is accepted as being self-evident. - Arthur Schopenhaue